Cybersecurity Guide

How to secure your industrial remote access according to NIS2 and IEC 62443

A Guide to configuring Ewon Talk2m and devices for NIS2 compliance using the ISA/IEC 62443 framework

Contents

1. Introduction 03

1.1 NIS2 DIRECTIVE CONSIDERATIONS 03

1.2 SUPPLY CHAIN RESPONSIBILITIES 04

2. Best practices for secure remote access 05

2.1 INTRODUCTION 05

2.2 ISA/IEC 62443 06

2.3 KEY AREAS WHERE IEC 62443 ALIGNS WITH NIS2 07

2.4 REMOTE ACCESS TO INDUSTRIAL ASSETS AND NIS2 08

2.5 EWON SOLUTIONS ADDRESSED IN THIS DOCUMENT 08

3. Controls and measures 09

3.1 ENSURE THE STRENGTH OF AUTHENTICATION IS APPROPRIATE 09

3.2 USE MULTI-FACTOR AUTHENTICATION 10

3.3 CHANGE OF AUTHENTICATION CREDENTIALS INITIALLY 12

3.4 IMPLEMENT AUTHENTICATION PROCEDURES BASED ON LEAST PRIVILEGE PRINCIPLE 13

3.5 REQUIRE THE RESET OF AUTHENTICATION CREDENTIALS AND THE BLOCKING OF USERS AFTER A PREDEFINED NUMBER OF UNSUCCESSFUL LOG-IN ATTEMPTS 14

3.6 ALLOW CONNECTIONS OF SERVICE PROVIDERS ONLY AFTER AN AUTHORIZATION REQUEST 15

3.7 USE TOOLS TO MONITOR AND LOG ACTIVITIES 16

3.8 NETWORK SEGMENTATION 18

3.9 SECURITY PATCH MANAGEMENT 26

3.10 DEACTIVATE UNNEEDED CONNECTIONS AND SERVICES 28

3.11 PROTECTION AGAINST UNAUTHORIZED SOFTWARE 29

3.12 ALLOW ACCESS TO THE NETWORK ONLY TO AUTHORIZED DEVICES 30

3.13 ESTABLISH, IMPLEMENT AND APPLY A POLICY AND PROCEDURES RELATED TO CRYPTOGRAPHY 32

3.14 APPLICATIONS USED IN THE AUTOMATION SOLUTION ARE COMMONLY ACCEPTED BY BOTH THE SECURITY AND INDUSTRIAL AUTOMATION COMMUNITIES 32

3.15 DETERMINE AND APPLY CONTROLS FOR REMOTE ACCESS TO IACS 34

3.16 REGULARLY REVIEW THE IDENTITIES AND, IF NO LONGER NEEDED, DEACTIVATE THEM WITHOUT DELAY 34

3.17 MAINTAIN POLICIES FOR MANAGEMENT OF PRIVILEGED AND SYSTEM ADMINISTRATION ACCOUNTS 35

4. Conclusion 36

Annex A - Mapping of NIS2 to IEC62443 and NIST 37

1. Introduction

As industrial environments become increasingly connected, the need for **secure remote access** has never been more critical. Remote access enables efficient monitoring, diagnostics, and maintenance, but it also introduces cybersecurity risks that must be addressed with a **robust security framework.** Additionally, in EU compliance with **NIS2 Directive** has become a key consideration, requiring organizations to adopt strict security measures.

Secure remote access to industrial systems is crucial, yet organizations face several significant challenges:

As industrial environments become increasingly connected, the need for secure remote access has never been more critical. Remote access enables efficient monitoring, diagnostics, and maintenance, but it also introduces cybersecurity risks that must be addressed with a robust security framework. Additionally, in EU compliance with NIS2Directive has become a key consideration, requiring organizations to adopt strict security measures.

Secure remote access to industrial systems is crucial, yet organizations face several significant challenges:

1. Cyber threats – Industrial systems are prime targets for cyberattacks, including unauthorized access, ransomware, and data breaches.

2. Legacy equipment – Many operational technology (OT) systems were not designed with security in mind, making them vulnerable to modern threats.

3. Compliance & Regulations – Standards like the ISA/IEC 62443, NIST 800-82, and ISO 27001 require strict controls for remote access security.

4. Reliability & Performance – Secure remote access must not introduce latency or disruptions in industrial processes.

1.1 NIS2 DIRECTIVE CONSIDERATIONS

The **NIS2 Directive**[1] specifically enforces stricter cybersecurity regulations for essential and important entities, including asset owners. Key security requirements include:

1. Risk-Based security controls – Organizations must implement robust risk management strategies for securing remote access.

2. Incident reporting obligations – Mandatory reporting of cybersecurity incidents affecting industrial environments.

3. Third-party security assurance – Machine Builders must ensure their solutions meet asset owners' security requirements and NIS2 compliance.

4. Network and information system security measures – Companiesmust protect remote access solutions against unauthorized access, cyber threats, and potential disruptions.

The **COMMISSION IMPLEMENTING REGULATION (EU)**[2] outlines more concrete what is expected of those companies that need to be compliant. Machine builders need to take these requirements into account and build them in by design – or make them easily adjustable to ensure simplified compliance for their customers.

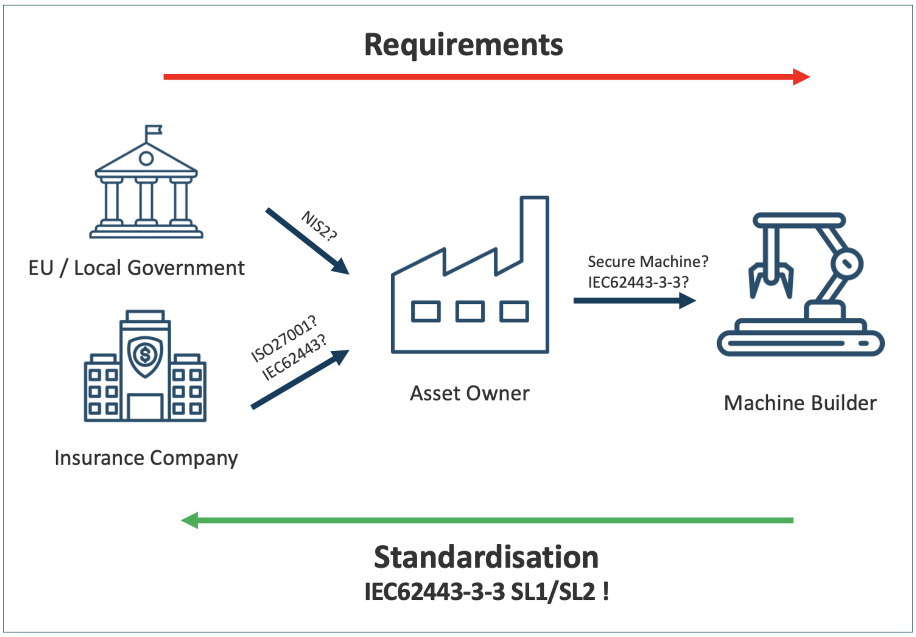
[1] https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

[2] https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks

1.2 SUPPLY CHAIN RESPONSIBILITIES

With the introduction of NIS2, asset owners have become responsible also to ensure that their supply chain is secure with the deliveries critical to the organization. These together with requirements from the insurance companies requesting clarification on the maturity of the cybersecurity work raise many questions with asset owners. One result of this is that procurement changes requesting a clear "secure-by-design" delivery. Machine builders need to adjust their architecture to answer these new requirements.

Fortunately, ISA/IEC 62443 provides good guidance for both policies and procedures in ISA/IEC 62443-2-4 where security program requirements are described as well as 62443-3-3 where system level technical requirements are outlined. Implementing and referring to these requirements will not only significantly increase the security of the machine but simplify the communication of security level included by design.



2. Best practices for secure remote access

2.1 INTRODUCTION

Remote access solutions available can be configured in various ways providing different security postures. Machine builders and end users should follow best practices for configuring and pushing the service. Best practices required by NIS2 and it's complementing guidelines by the commission implementing regulation for Secure Remote Access in Industrial Environments include:

1. Ensure the strength of authentication is appropriate.
2. Use multi-factor authentication.
3. Change of authentication credentials initially.
4. Implement authentication procedures based on least privilege principle.
5. Require the reset of authentication credentials and the blocking of users after a predefined number of unsuccessful log-in attempts.
6. Allow connections of service providers only after an authorization request.
7. Use tools to monitor and log activities.
8. Network segmentation & configure controls to prevent unnecessary access.
9. Security patch management.
10. Deactivate unneeded connections and services.
11. Protection against unauthorized software.
12. Only allow authorized devices to access thenetwork.
13. Establish, implement and apply a policy and procedures related to cryptography.
14. Applications used in the automation solution are widely accepted by both the security and industrial automation communities.
15. Determine and apply controls for remote access to IACS.
16. Regularly review the identities and, if no longer needed, deactivate them without delay.
17. Maintain policies for management of privileged and system administration accounts.

Implementing these requirements significantly enhances cybersecurity, operational stability, and compliance in industrial environments. To clearly communicate and adopt best practices, it's beneficial to refer to recognized standards and pursue compliance. Since industrial remote access intersects IT and OT systems, and spans both on-premises and cloud environments, a combination of standards is recommended. For IT security related to services and information management, ISO 27001 is widely recognized as the industry's best practice.

Meanwhile, for OT security concerning machines and devices, ISA/IEC 62443 provides the standard guidelines.

2.2 ISA/IEC 62443

IEC 62443 is an international set of standards focused on cybersecurity for industrial automation and control systems (IACS). IEC 62443-2-4 defines what service providers (like system integrators or vendors) must do to securely design, implement, and maintain industrial automation systems for their customers.

- **Secure engineering practices →** Following cybersecurity best practices during system design and integration

- **System hardening and configuration →** Ensuring systems are delivered with secure settings, proper patching, and minimal attack surface.

- **User management & access control →** Making sure user roles and permissions are clearly defined and enforced.

- **Remote access security →** Secure ways for service providers to access systems for maintenance or updates.

- **Auditability & documentation →** Tracking what was done, when, and by whom — and making that information available to the end customer.

IEC 62443-3-3 is another core part of the same cybersecurity standard family, but it focuses on system-level technical requirements. It defines what technical controls a system must have to achieve a certain security level (SL1 to SL4). Each control is applied depending on the threat environment. There are four security levels:

- **SL 1:** Protection against casual or accidental misuse.
- **SL 2:** Protection against intentional misuse with simple tools.
- **SL 3:** Protection against sophisticated attackers with moderate resources.
- **SL 4:** Protection against highly skilled attackers with significant resources.

The standard is structured in detailed requirements grouped into seven foundational requirements (FRs):

1. **Identification & Authentication Control (IAC) →** Who's accessing the system? Are they authenticated?
2. **Use Control (UC) →** What are users allowed to do?
3. **System Integrity (SI) →** Protection against unauthorized changes or malware.
4. **Data Confidentiality (DC) →** Encryption and protection of sensitive data.
5. **Restricted Data Flow (RDF) →** Limiting communication paths (e.g., firewalls, segmentation).
6. **Timely Response to Events (TRE) →** Logging, alerts, and incident handling.
7. **Resource Availability (RA) →** Keeping the system up and running, even under attack (e.g., DoS protection).

Following the IEC 62443 standards as a reference framework and documenting the protection measures you implement is a highly effective and structured approach to designing and securing a machine or industrial system. This method provides clear guidance, enhances consistency and quality, facilitates risk assessment, simplifies documentation and audits, and supports both compliance and communication. You're not starting from scratch- IEC 62443 offers a well-defined set of security requirements and best practices.

2.3 KEY AREAS WHERE IEC 62443 ALIGNS WITH NIS2

The ISA/IEC 62443 framework provides a structured approach that enables organizations to meet the obligations set forth by NIS2. By following the principles outlined in IEC 62443, any organization can enhance its cyber security posture and navigate the complexities of risk management effectively.

Below are the five key areas where IEC 62443 aligns with NIS2:

1. Risk management & Security measures

NIS2 requirement: entities must implement risk-based security measures.

IEC 62443-2-1	Outlines cybersecurity risk management programs.
IEC 62443-3-2	Helps assess risk and define security levels for industrial systems.
IEC 62443-4-2	Provides security requirements for individual components.

2. Supply chain security

NIS2 requirement: organizations must ensure their supply chains are secure.

IEC 62443-2-4	Defines security requirements for service providers (e.g., integrators, vendors).
IEC 62443-4-1	Sets security guidelines for secure product development.
IEC 62443-3-3	Enforces security controls for systems and networks.

3. Incident reporting & response

NIS2 requirement: mandatory reporting of security incidents within 24 hours (initial report) and 72 hours (detailed report) to national authorities.

IEC 62443-2-1	Requires asset owners to have incident response and recovery plans.
IEC 62443-2-4	Requires service providers to have incident response and recovery plans.

4. Access control & Identity management

NIS2 requirement: strong access controls and identity management.

IEC 62443-3-3	Enforces security controls for systems and networks.
IEC 62443-4-2	Provides security requirements for individual components.

5. Business continuity & Resilience

NIS2 requirement: organizations must ensure operational continuity during cyber incidents.

IEC 62443-2-1	Requires backup, disaster recovery, and business continuity planning for IACS environments by asset owners.
IEC 62443-2-4	Requires backup, disaster recovery, and business continuity planning for IACS environments by service providers.

2.4 REMOTE ACCESS TO INDUSTRIAL ASSETS AND NIS2

This document further discusses the Ewon secure remote access product and Talk2m service, detailing proper configuration to align with established best practices according to ISA/IEC 62443. It also serves as a practical reference guide for meeting the requirements of the NIS2 directive.

2.5 EWON SOLUTIONS ADDRESSED IN THIS DOCUMENT

Talk2m

Ewon Talk2m[3] is a secure Industrial cloud service developed by HMS Networks[2]. It is widely used for secure VPN connections between remote users (engineers, technicians) and industrial devices such as PLCs, HMIs, and SCADA systems

More information at https://www.hms-networks.com/software-and-tools/Talk2m

Ecatcher

Ewon Ecatcher[4] is the VPN client software used to connect securely to remote industrial devices via Ewon Talk2m. It is developed by HMS Networks and allows users to establish encrypted VPN connections with industrial machines equipped with Ewongateways (e.g. Ewon Cosy, Ewon Flexy).

Ewon Cosy+

The Ewon Cosy+[5] is an industrial VPN gateway designed for secure remote access to machines and industrial equipment. It enables OEMs, machine builders, and system integrators to remotely troubleshoot and maintain PLCs, HMIs, and other automation devices without requiring on-site visits.

More information at https://www.hms-networks.com/support/remote-gateways

Ewon Flexy

Ewon Flexy[6] is a flexible industrial IoT gateway that provides secure remote access, data logging, and cloud connectivity for industrial machines. It is ideal for OEMs, system integrators, and manufacturers who need both remote troubleshooting and advanced IIoT capabilities such as predictive maintenance and real-time

[3] https://www.hms-networks.com/software-and-tools/Talk2m/Talk2m-pro
[4] https://www.hms-networks.com/Ecatcher
[5] https://www.hms-networks.com/p/ec71330-00ma-ewon-cosy-ethernet
[6] https://www.hms-networks.com/p/flexy20500-00ma-ewon-flexy-205

3. Controls and measures

3.1 ENSURE THE STRENGTH OF AUTHENTICATION IS APPROPRIATE

Category: Access control

Why it matters?

Strong authentication not only safeguards privacy but also ensures regulatory compliance, fosters trust among stakeholders, and supports business continuity by reducing the risk of security breaches.

To enhance the security of your systems, it is imperative to implement clear policies and procedures that focus on password management. This includes enforcing complexity requirements to create stronger passwords, limiting the reuse of passwords to avoid vulnerabilities, and defining expiration periods to ensure that passwords are regularly updated.

By prioritizing these authentication measures, organizations can significantly strengthen their security posture and protect sensitive information from potential threats. Effective authentication is the first line of defense in maintaining the integrity of your industrial control systems.

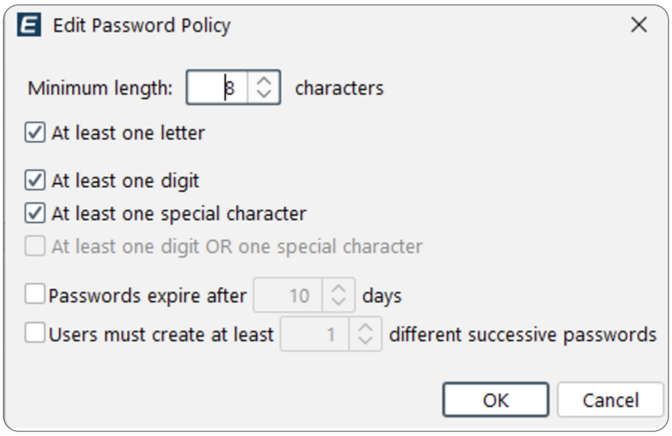
What to do according to ISA/IEC 62443

Standard	ISA/IEC 62443-2-4
Req ID	SP.09.05
Implement password policies that meet a minimum complexity standard widely recognized by both the security and industrial automation sectors, with minimal password complexity as follows: 1. At least eight characters in length and 2. A combination of at least three of the following four character sets: lowercase, uppercase, numeric digit, and special characters (e.g.% and #).	

Standard	ISA/IEC 62443-3-3
System Requirement	SR1.7
The control system shall enforce configurable password strength based on minimum length and variety of character types.	

How to configure Ewon

With Ecatcher you should define the strength password policy of a Talk2m account:



Edit Password Policy

Minimum length: 8 characters

☑ At least one letter

☑ At least one digit

☑ At least one special character

□ At least one digit OR one special character

□ Passwords expire after 10 days

□ Users must create at least 1 different successive passwords

Set a minimum of 8 characters to comply with IEC 62443 and also consider NIST Special Publication 800-63B, which specifies a minimum of 8 characters and suggests at least 15 characters for enhanced security. Ewon supports setting a length of up to 45 characters – a good best practice is to make up a sentence that is easy to remember but long, and therefor hard to crack.

More information available at https://help.ewon.biz/Ecatcher/help/en/account-498351.html

3.2 USE MULTI-FACTOR AUTHENTICATION

Category: Access control

Why it matters?

Implementing Multi-Factor Authentication (MFA) for industrial control systems is crucial in safeguarding valuable assets from various cyber threats, unauthorized access, and potential operational disruptions. By utilizing MFA, organizations can enhance their security posture, as it introduces an additional layer of authentication beyond just passwords. Thismeans that even if passwords are compromised, unauthorized individuals will still be unable to access sensitive systems without the necessary secondary verification.

MFA ensures that only authorized personnel can gain entry to critical systems, significantly reducing the risk of security breaches As cyberattacks become increasingly sophisticated, relying solely on traditional password-based authentication is no longer sufficient. Adopting MFA not only fortifies security measures but also instills greater confidence in the integrity of industrial operations.

In summary, incorporating Multi-Factor Authentication is an essential strategy for enhancing security in industrial control systems, effectively safeguarding against unauthorized access, and protecting against the

What to do according to ISA/IEC 62443

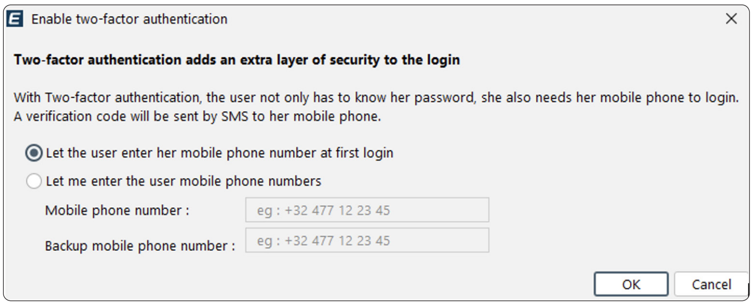
Standard	ISA/IEC 62443-2-4
Req ID	SP.03.07 RE(1)
Applies to	The service provider
Use Multi-Factor Authentication as required by the asset owner.	

What to do according to ISA/IEC 62443

Standard	ISA/IEC 62443-3-3
Req ID	SR1.1 RE(2)
Applies to	The system configuration
Employ Multi-Factor Authentication for human user access to the control system via an untrusted network.	

How to configure Ewon

Within Ecatcher, administrators can enable and configure two-factor authentication settings for each user on the Talk2m account. This option is not enabled by default. When a user with two-factor authentication logs into Ecatcher or M2web, a verification code is sent via SMS to their mobile phone. It is also possible to allow the user, on their first login, to provide the mobile number that will be used to receive SMS security codes.



Enable two-factor authentication

Two-factor authentication adds an extra layer of security to the login

With Two-factor authentication, the user not only has to know her password, she also needs her mobile phone to login. A verification code will be sent by SMS to her mobile phone.

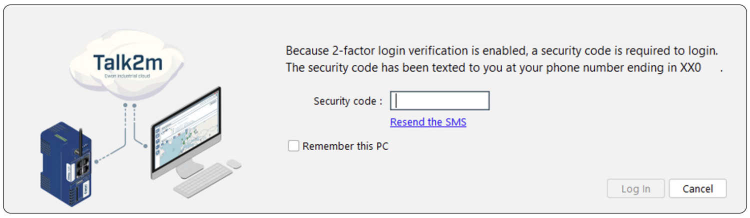
● Let the user enter her mobile phone number at first login

○ Let me enter the user mobile phone numbers

Mobile phone number : eg : +32 477 12 23 45

Backup mobile phone number : eg : +32 477 12 23 45

When a user logs into the Talk2m account, they will first need to enter their username and password. The Talk2m system will then send a dynamic, one-time authorization passcode (consisting of 4 digits) to their cell phone, which serves as second factor. To complete the login process, the user will need to enter the code inside the 'Security Code' field.



Because 2-factor login verification is enabled, a security code is required to login.
The security code has been texted to you at your phone number ending in XX0 .

Security code :

□ Remember this PC

The user has three attempts to enter the correct code. After three failed attempts the login will be temporarily blocked.

A prerequisite for using two-factor authentication is that all accounts must be named, and usernames should never be shared. Each account must have a mobile phone number registered on the Talk2m platform.

Only administrators are authorized to change the mobile phone number once it has been set.

For more information, visit https://help.ewon.biz/Ecatcher/help/en/users.html#two-factor-authentication-495175

3.3 CHANGE OF AUTHENTICATION CREDENTIALS INITIALLY

Category: Access control

Why it matters?

By replacing default or easily guessable passwords- often found in publicly available instruction manuals - you significantly reduce the risk of unauthorized access. This proactive measure ensures that only authorized users have control from the very beginning, thereby enhancing security. Also, credentials must be changed when there is a suspicion that the credential has been revealed to an unauthorized person.

Absolutely nothing should be accessible via “guest” or anonymous accounts.

What to do according to ISA/IEC 62443

Standard	ISA/IEC 62443-2-4
Req ID	SP.09.07
Applies to	The service provider
Change the default passwords as required by the asset owner.	

Standard	ISA/IEC 62443-3-3
System Requirement	SR1.5
Applies to	The system configuration
Configuring the authenticators is as follows: a) Initialize the authenticator content; b) Change all default authenticators upon control system installation; c) Change/refresh all authenticators regularly; and d) Protect all authenticators from unauthorized disclosure and modification when stored and transmitted.	

How to configure Ewon

Talk2m

There are no default passwords in Talk2m. When creating an account or a user for the first time, both the username and password must be created.

Ewon Cosy+

By default, you will be asked to change the password initially.

Ewon Flexy

By default, Ewon Flexy series are shipped with a unique password. You must ensure that you change it initially.

3.4 IMPLEMENT AUTHENTICATION PROCEDURES BASED ON LEAST PRIVILEGE PRINCIPLE

Category: Access control

Why it matters?

Least Privilege is a guiding principle of Zero Trust that ensures users, applications, and systems are granted only the minimal access or permissions necessary to perform their designated tasks. By limiting access rights, this principle helps prevent both accidental and intentional misuse of privileges, thereby significantly reducing the risk of security breaches.

Additionally, it serves as a barrier against the spread of malware, as unauthorized access is limited, minimizing the potential impact of any security vulnerabilities. To implement this principle effectively, robust authentication measures are required to verify the identity of users and systems before granting access.

What to do according to ISA/IEC 62443

Standard	ISA/IEC 62443-2-4
Req ID	SP.03.08
Applies to	The service provider
This requirement is about ensuring that least privilege is used for the administration of network devices for which the service provider is responsible	

Standard	ISA/IEC 62443-3-3
System Requirement	SR2.1
Applies to	The system configuration
The systems shall be protected on all interfaces and provide the capability to enforce authorizations for all human users, supporting segregation of duties and the principle of least privilege.	

How to configure Ewon

Users should only have access to information or permissions necessary to undertake their duties, on a need-to-know basis.

Configure the Ewon system based on the Least Privilege principle. As an administrator, you can define which users have access to which Ewon gateways, as well as what rights users have regarding user management and device management[7]

- Most users should be defined as standard users with limited permissions.

- Use the «user group» feature of the Talk2m account to define user profiles to which specific permissions, access rights and/or management roles are attributed. For example, it is possible to restrict the access rights of a group of users to only specific Ewon gateways, or even to specific devices connected behind these Ewon gateways.

- Administrators have the responsibility of managing the rights and permissions of other users and as such, this duty should be limited to highly trusted personnel within the organization.

- Limited administrative roles can be attributed to some users, with the authority to manage specific groups of users or pools of devices.

[7] Only available in Talk2m pro

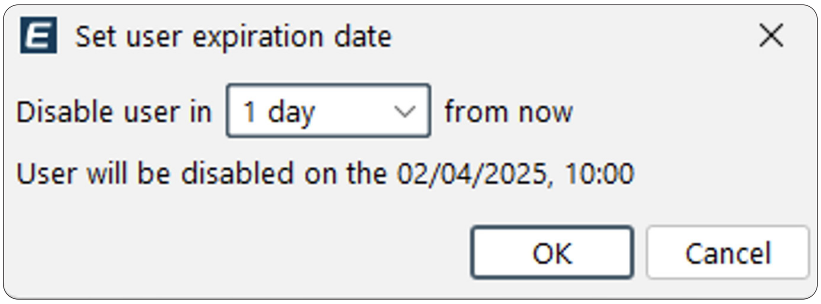
In Talk2m, users belong to groups. A user group defines which rights the user will have on other user groups and/or on Ewon pools[8].

User groups define the access rights that member users have on different Ewon pools as well as what administrative roles users have on the account, their own user group, and otheruser groups. Every user must belong to at least one user group.

Shared user accounts should be avoided under all circumstances, as they prevent accountability and lead to major security issues when an employee leaves the company. Create a unique user for each person interacting with the Ewon solution.

Also, to further strengthen security, administrators of the Talk2m account can keep users disabled by default with the "User temporary activation". With this function, it is possible to enable users of the Talk2m account only when they need to perform a task, such as a remote maintenance operation on a machine, and disable them once their task is done.

To make a user temporary, go to 'user properties' and set 'user expiration date'.



Set user expiration date

Disable user in 1 day from now

User will be disabled on the 02/04/2025, 10:00

For more information visit https://hmsnetworks.blob.core.windows.net/nlw/docs/default-source/products/ewon/application-notes/aug-0086-00-manage-device-access-with-Talk2m-pro-account.pdf

3.5 REQUIRE THE RESET OF AUTHENTICATION CREDENTIALS AND THE BLOCKING OF USERS AFTER A PREDEFINED NUMBER OF UNSUCCESSFUL LOG-IN ATTEMPTS

Category: Access control

Why it matters?

A Failed Login Attempt refers to an instance when a user tries to access their account but is unable to do so successfully. To enhance security, systems monitor these attempts. If a user surpasses a specified number of failed login attempts, their account will be automatically locked for a predetermined duration. This proactive measure is crucial in safeguarding against unauthorized access and significantly reduces the risk of brute-force attacks, where malicious actors try to gain entry by guessing passwords.

[8] Ewon pools are collections of Ewon gateways

What to do according to ISA/IEC 62443

Standard	ISA/IEC 62443-3-3
System Requirement	SR1.11
Applies to	The system configuration
This requirement enforces a limit of a configurable number of consecutive invalid access attempts by the user during a configurable time period. Access will be denied for a specified period of time or until unlocked by an administrator when this limit has been exceeded.	

How to configure Ewon

Ewon Talk2m login provides this functionality by default, locking the access of a user for 15 minutes when an incorrect password has been used 10 consecutive times, following the recommendation of NIST 800-63B[9].

3.6 ALLOW CONNECTIONS OF SERVICE PROVIDERS ONLY AFTER AN AUTHORIZATION REQUEST

Category: Access control

Why it matters?

This function plays a vital role in maintaining security, as it guarantees that a remote connection can only be established with the explicit authorization of the asset owner and may be limited to a predetermined duration. This ensures that access is granted only under specific conditions, such as when the machine is idle or functioning in a secure operating mode. By requiring prior authorization, the system is better equipped to identify and flag any unauthorized connections, which could indicate potential attacks.

What to do according to ISA/IEC 62443

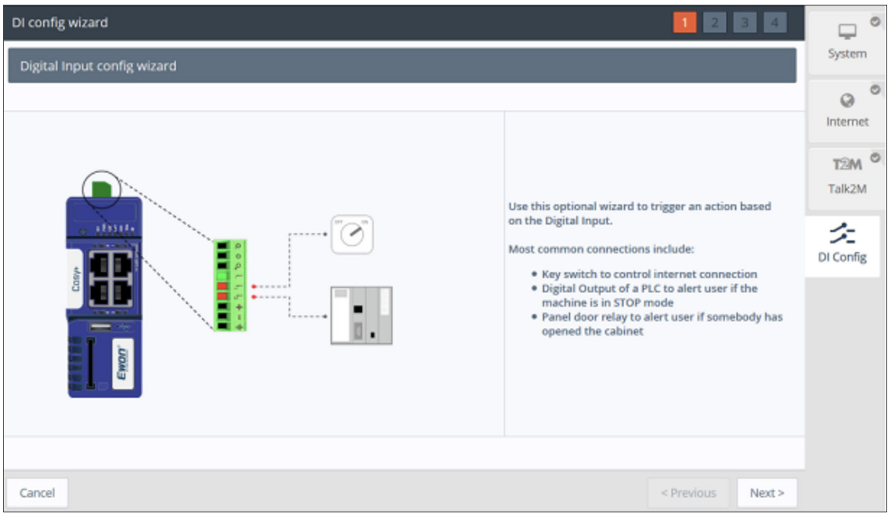
Standard	ISA/IEC 62443-2-4
Req ID	SP.07.04
Applies to	The service provider
The service provider shall have the capability to ensure that it obtains approval from the asset owner prior to using each and every remote access connection.	

Standard	ISA/IEC 62443-3-3
System Requirement	SR1.13 RE(1)
Applies to	The system configuration
An assigned role must approve access via untrusted networks.	

[9] https://pages.nist.gov/800-63-3/sp800-63b.html

How to configure Ewon

To guarantee that the asset owner retains full control over remote access, Ewon gateways provide a feature that requires the owner's approval for each connection. With this functionality, the asset owner activates the permission, as Ewon gateways can be configured to enable or restrict remote access based on the state of a digital input.



Use this optional wizard to trigger an action based on the Digital Input.

Most common connections include:

- Key switch to control internet connection
- Digital Output of a PLC to alert user if the machine is in STOP mode
- Panel door relay to alert user if somebody has opened the cabinet

The asset owner must activate the digital input to grant authorization; otherwise, a remote connection cannot be established. Common methods for activating this input include:

1. With a physical switch activated manually.
2. With an operator or automatic action from the SCADA or HMI (not for Ewon Cosy+).
3. With an automatic output from the PLC (for instance, time or condition based).
4. With a script in the Ewon (not for Ewon Cosy+).

While the connection is active, a digital output in the Ewon gateway is automatically triggered to inform the asset owner that remote access is in progress - an essential safety measure. Additionally, both the digital input and digital output status are recorded in the Talk2m report (see 3.7).

3.7 USE TOOLS TO MONITOR AND LOG ACTIVITIES

Category: Incident handling

Why it matters?

Monitoring is crucial as it enables the detection of unauthorized access, anomalies, and potential cyber threats. By actively overseeing system activities, organizations can identify suspicious behavior before it escalates into a significant issue.

Logging serves as a critical resource, providing a comprehensive record of system activities that is invaluable for forensic investigations. This historical data not only aids in understanding the nature of a security incident but also helps organizations comply with various security regulations. By maintaining thorough logs, companies can demonstrate adherence to industry standards and enhance their overall security posture.

What to do according to ISA/IEC 62443

Standard	ISA/IEC 62443-2-4
Req ID	SP.08.02
Applies to	The service provider
The service provider shall ensure that the automation solution is configured to write all security-related events, including user activities and account management activities, to an audit log that is kept for the number of days specified by the asset owner.	

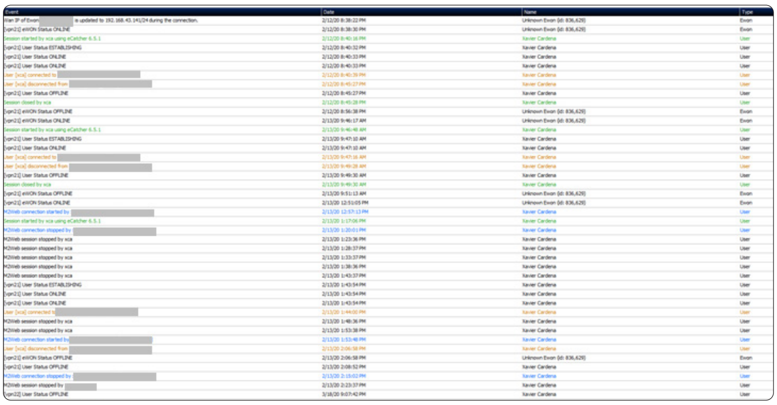
Standard	ISA/IEC 62443-3-3
System Requirement	SR2.8
Applies to	The system configuration
The control system shall generate audit records relevant to security for the following categories: access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance activity and audit log events. Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.	

How to configure Ewon

A Connection Log Report is available in Talk2m which includes the following information:

- The day and time the event occurred.
- The name of the Ewon or user triggering the event.
- Whether this event was triggered by an Ewon or a user.
- The event itself (connection/disconnection of user, wake up of an Ewon...).

The Connection Log Report shows who connected, when, at what time, for how long, and to which machine. Optionally, with the Logbook function, it is possible to leave a message or a trace of what has been done while the connection to the Ewon. This can be the actions performed on the Ewon or the devices connected to it, a reminder of what needs to be done the next time, a remark for a specific user, etc. Examples can be changes in the PLC program, troubleshooting, etc.



Event	Date	Name	Type
Wan IP of Ewon [redacted] is updated to 192.168.43.141/24 during the connection.	2/12/20 8:38:22 PM	Unknown Ewon (id: 836,629)	Ewon
[vpn21] eWON Status ONLINE	2/12/20 8:38:30 PM	Unknown Ewon (id: 836,629)	Ewon
Session started by xca using eCatcher 6.5.1	2/12/20 8:40:16 PM	Xavier Cardena	User
[vpn21] User Status ESTABLISHING	2/12/20 8:40:32 PM	Xavier Cardena	User
[vpn21] User Status ONLINE	2/12/20 8:40:33 PM	Xavier Cardena	User
[vpn21] User Status ONLINE	2/12/20 8:40:33 PM	Xavier Cardena	User
User [xca] connected to [redacted]	2/12/20 8:40:39 PM	Xavier Cardena	User
User [xca] disconnected from [redacted]	2/12/20 8:45:27 PM	Xavier Cardena	User
[vpn21] User Status OFFLINE	2/12/20 8:45:27 PM	Xavier Cardena	User
Session closed by xca	2/12/20 8:45:28 PM	Xavier Cardena	User
[vpn21] eWON Status OFFLINE	2/12/20 8:56:38 PM	Unknown Ewon (id: 836,629)	Ewon
[vpn21] eWON Status ONLINE	2/13/20 9:46:17 AM	Unknown Ewon (id: 836,629)	Ewon
Session started by xca using eCatcher 6.5.1	2/13/20 9:46:48 AM	Xavier Cardena	User
[vpn21] User Status ESTABLISHING	2/13/20 9:47:10 AM	Xavier Cardena	User
[vpn21] User Status ONLINE	2/13/20 9:47:10 AM	Xavier Cardena	User
User [xca] connected to [redacted]	2/13/20 9:47:16 AM	Xavier Cardena	User
User [xca] disconnected from [redacted]	2/13/20 9:49:28 AM	Xavier Cardena	User
[vpn21] User Status OFFLINE	2/13/20 9:49:30 AM	Xavier Cardena	User
Session closed by xca	2/13/20 9:49:30 AM	Xavier Cardena	User
[vpn21] eWON Status OFFLINE	2/13/20 9:51:13 AM	Unknown Ewon (id: 836,629)	Ewon
[vpn21] eWON Status ONLINE	2/13/20 12:51:05 PM	Unknown Ewon (id: 836,629)	Ewon
M2Web connection started by [redacted]	2/13/20 12:57:13 PM	Xavier Cardena	User
Session started by xca using eCatcher 6.5.1	2/13/20 1:17:06 PM	Xavier Cardena	User
M2Web connection stopped by [redacted]	2/13/20 1:20:01 PM	Xavier Cardena	User
M2Web session stopped by xca	2/13/20 1:23:36 PM	Xavier Cardena	User
M2Web session stopped by xca	2/13/20 1:28:37 PM	Xavier Cardena	User
M2Web session stopped by xca	2/13/20 1:33:37 PM	Xavier Cardena	User
M2Web session stopped by xca	2/13/20 1:38:36 PM	Xavier Cardena	User
M2Web session stopped by xca	2/13/20 1:43:37 PM	Xavier Cardena	User
[vpn21] User Status ESTABLISHING	2/13/20 1:43:54 PM	Xavier Cardena	User
[vpn21] User Status ONLINE	2/13/20 1:43:54 PM	Xavier Cardena	User
[vpn21] User Status ONLINE	2/13/20 1:43:54 PM	Xavier Cardena	User
User [xca] connected to [redacted]	2/13/20 1:44:00 PM	Xavier Cardena	User
M2Web session stopped by xca	2/13/20 1:48:36 PM	Xavier Cardena	User
M2Web session stopped by xca	2/13/20 1:53:38 PM	Xavier Cardena	User
M2Web connection started by [redacted]	2/13/20 1:53:48 PM	Xavier Cardena	User
User [xca] disconnected from [redacted]	2/13/20 2:06:58 PM	Xavier Cardena	User
[vpn21] eWON Status OFFLINE	2/13/20 2:06:58 PM	Unknown Ewon (id: 836,629)	Ewon
[vpn21] User Status OFFLINE	2/13/20 2:08:52 PM	Xavier Cardena	User
M2Web connection stopped by [redacted]	2/13/20 2:15:02 PM	Xavier Cardena	User
M2Web session stopped by [redacted]	2/13/20 2:23:37 PM	Xavier Cardena	User
[vpn22] User Status OFFLINE	3/18/20 9:07:42 PM	Xavier Cardena	User

The list of events can be exported as CSV for analysis.

More information is available at https://help.ewon.biz/Ecatcher/help/en/ewons.html

3.8 NETWORK SEGMENTATION

Category: Network security

Why it matters?

Segmenting networks within an Industrial Control System (ICS) significantly mitigates the risk of cyber threats propagating through critical systems. By separating operational technology (OT) from IT networks, and OT networks from each other, network segmentation effectively limits unauthorized access, contains potential attacks, and bolsters threat detection capabilities. It both helps prevent malicious actors from getting in, but it also reduces the impact by limiting spreading if an incident does occur.

Moreover, proper segmentation not only fortifies security, but also improves overall system reliability and minimizes operational disruptions. This practice aligns with established cybersecurity best practices and meets various regulatory requirements, ensuring that organizations adhere to necessary standards for safeguarding their infrastructure.

What to do according to ISA/IEC 62443

Standard	ISA/IEC 62443-2-4
Req ID	SP.03.02
Applies to	The service provider
The service provider shall have the capability to ensure that the physical network segmentation architecture used in the automation solution, including its use of network security devices or equivalent mechanisms, is implemented according to the automation solution design approved by the asset owner.	

Standard	ISA/IEC 62443-2-4
System Requirement	SP.03.02 RE(1)
Applies to	The service provider
The service provider shall have the capability to identify and document the network segments of the automation solution and their interfaces to other segments, including external networks. For each interface, the provider shall designate whether it is trusted or untrusted.	

Standard	ISA/IEC 62443-2-4
Req ID	P.03.02 RE(2)[10]
Applies to	The service provider

The service provider shall have the capability to ensure that interfaces of the automation solution that have been identified as untrusted are protected by network security devices or equivalent mechanisms, with documented and maintained security rules. At a minimum, the following shall be protected:

1. External interfaces.
2. Level 2/Level 3 interfaces[11].
3. Interfaces between the BPCS and the SIS.
4. Interfaces connecting wired and wireless BPCS networks.
5. Interfaces connecting the BPCS to data warehouses (e.g. enterprise historians).

Standard	ISA/IEC 62443-3-3
System Requirement	SR5.1 for SL1 and SR5.1(1) for SL2
Applies to	The system configuration

IEC 62443-3-3 defines system-level technical requirements for network segmentation and access control, aligned with the desired Security Level (SL1–SL4). Depending on the target SL, different network architectures must be implemented to restrict and control traffic flow.

A security assessment - including a risk analysis - is required to divide the system into security zones, with conduits managing communication between them. A zone can represent a single machine, an entire production line, or just a part of a machine, based on the risk profile.

Common examples include:

- Control zone – for operational control systems.
- Safety zone – for safety-related functions.
- Untrusted zone – area outside the machine's perimeter, often not managed by the asset owner and considered higher risk.
- Supervisory zone- for higher-level systems like Engineering Workstations, SCADA, MES, or diagnostics.
- Enterprise zone- for systems on the corporate IT network (ERP, email, file servers)
- Demilitarized zone (DMZ) – a buffer zone between the enterprise network and the control/supervisory systems. Often used to securely host data historians, OPC servers, etc.

This zoning approach ensures that traffic is limited to only what's necessary, reducing the attack surface and supporting a defense-in-depth strategy.

For SL1 compliance, Logical Segmentation is specified as required in SR5.1, here VLANs can be sufficient.

For SL2 compliance, Physical Segmentation is specified as required in SR5.1(1), in these scenarios the zones must have dedicated layer 2 switch infrastructure and be connected with a firewall with dedicated physical NICs as segments.

[10] Note that according to SP.03.02 RE(2), "For some, responsibility for maintaining firewall rules and documentation transfers to the asset owner prior to or at automation solution turnover. In this case, the service provider's role may be, as required by the asset owner, only to support verification that the firewall rules are accurate and up-to-date

[11] Depending on the automation solution, Level 2/Level 3 interfaces may be "External" interface

<table>
<tr><td>Standard</td><td>ISA/IEC 62443-3-3</td></tr>
<tr><td>System Requirement</td><td>SR5.2 for SL1 and SR5.2(1) for SL2</td></tr>
<tr><td>Applies to</td><td>The system configuration</td></tr>
<tr><td colspan="2">For a SL1 compliance zone, boundary protection is required according to SR5.2. The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.
For a SL2 compliance Deny by default, allow by exception is required according to SR5.2. The control system shall provide the capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception).</td></tr>
</table>

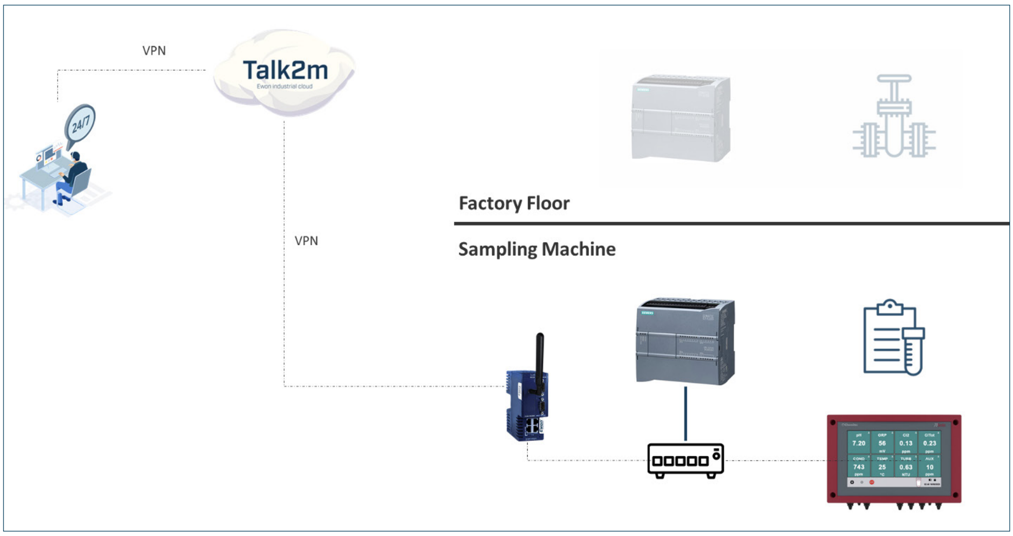
How to configure an Ewon gateway

The level of segmentation applied depends on the risk profile and the need for connectivity between the machine and the asset owners’ network. Below we consider 5 different scenarios:

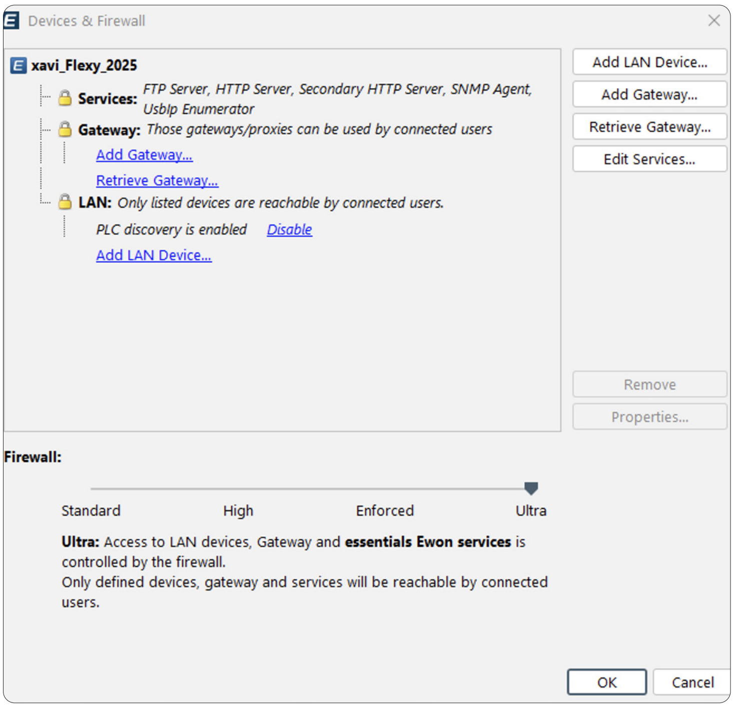
(1) Scenario 1: Ewon gateway in standalone machine configuration with Talk2m

Standalone machines, such as water pumps or quality measurement devices, often operate in isolated environments without connections to other systems. Machine builders typically require remote access to log in for maintenance or troubleshooting when indicated by visual alerts. In such cases, the machine is isolated within a single network segment, with the Ewon gateway serving as an edge gateway.

A threat analysis indicates potential risks if unauthorized parties compromise the remote access device, potentially allowing malicious traffic to reach the machine. Similarly, if a physical breach occurs on-site, unauthorized traffic might travel from the machine to the VPN client once the connection is established



To mitigate these risks, it is recommended to restrict the types of traffic allowed through the VPN connection. This restriction can be configured directly within Ecatcher. Traffic control and restriction capabilities are enforced through the Talk2m cloud service.



xavi_Flexy_2025

Services: *FTP Server, HTTP Server, Secondary HTTP Server, SNMP Agent, UsbIp Enumerator*

Gateway: *Those gateways/proxies can be used by connected users*

Add Gateway...

Retrieve Gateway...

LAN: *Only listed devices are reachable by connected users.*

PLC discovery is enabled *Disable*

Add LAN Device...

Firewall:

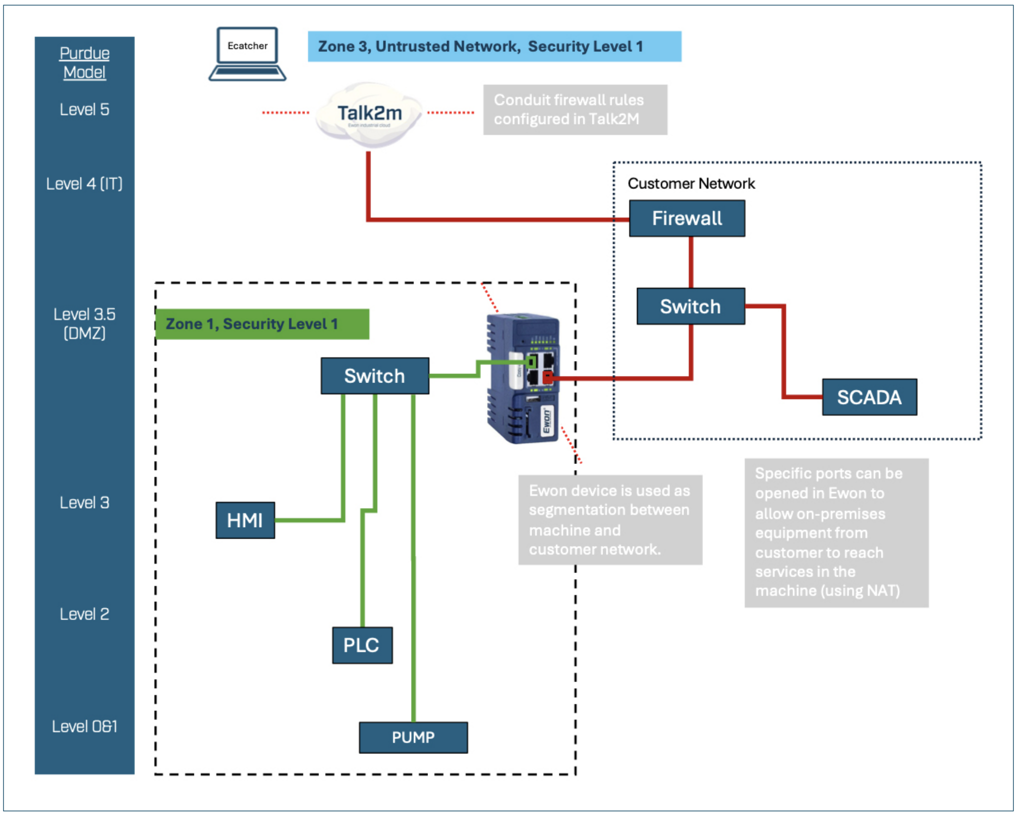
Standard High Enforced Ultra

Ultra: Access to LAN devices, Gateway and **essentials Ewon services** is controlled by the firewall.
Only defined devices, gateway and services will be reachable by connected users.

To mitigate these risks, it is recommended to restrict the types of traffic allowed through the VPN connection. This restriction can be configured directly within Ecatcher under Devices & Firewall. Traffic control and restriction capabilities are enforced in the Talk2m cloud service by configuring the “Firewall:” setting to “Ultra” [12].

(2) Scenario 2: Ewon as gateway for machine

A common setup can be that the Ewon gateway is used as the perimeter between the machine and the customers’ network. By default, the Ewon gateway will restrict all traffic from Customer to Machine network, from WAN to LAN. Traffic from Ecatcher to LAN must be restricted in the same way as for Scenario 1- configured in Ecatcher and deployed and enforced in Talk2m cloud.



Conduit firewall rules configured in Talk2M

Ewon device is used as segmentation between machine and customer network.

Specific ports can be opened in Ewon to allow on-premises equipment from customer to reach services in the machine (using NAT)

[12] Only available in Talk2m pro

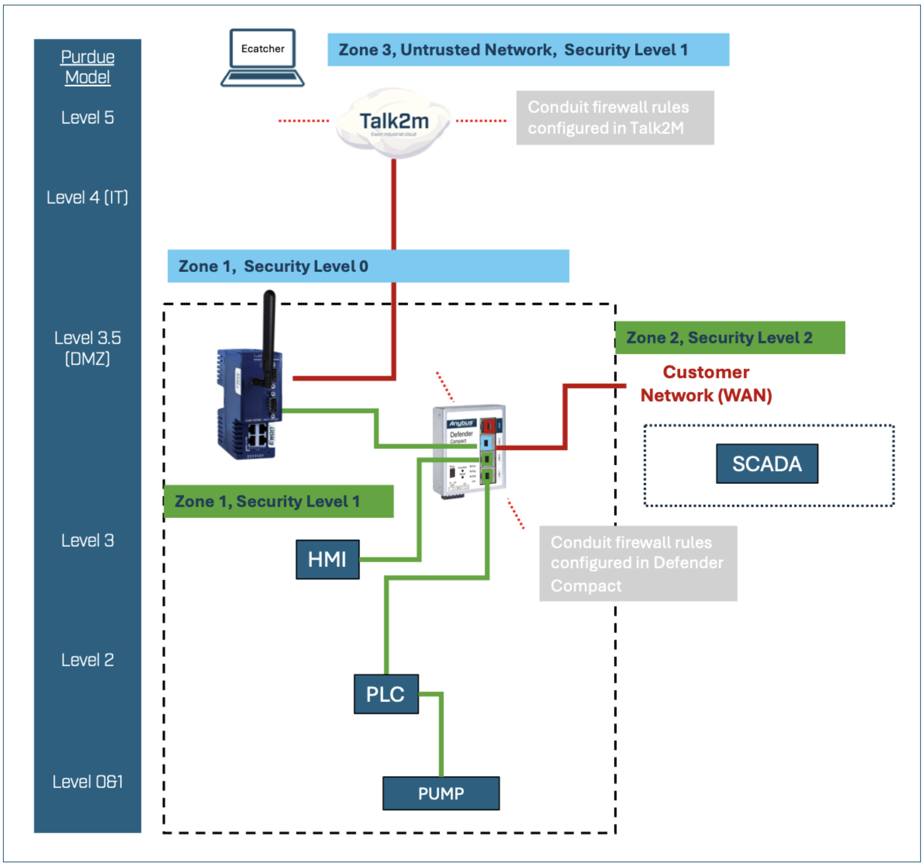
In Ewon Cosy+ or Ewon Flexy, configure WAN protection level: “Discard all traffic excepted VPN and initiated traffic (ex: Email)” must be set and this is enabled by default.

Setting up NAT 1:1 between WAN and LAN is possible to allow for instance the SCADA system to poll the PLC. The configuration will however open all TCP and UDP ports on such a 1:1 NAT traversal – increasing the threat surface significantly. It’s recommended to instead use a firewall with rules that restrict the type of traffic allowed over the NAT and apply port restrictions.

(3) Scenario 3: standalone machine requiring remote access and connectivity to asset owner’s network[13]

In situations where a standalone machine not only requires remote access but also connectivity to the asset owner’s internal network, a SCADA system or other operational tools may need to collect data from the machine. This ensures accurate status updates are communicated to plant operators, and local data extraction may also be necessary for additional purposes.

Within the machine, the Ewon gateway provides direct remote access and should be configured using firewall policies in the Talk2m cloud like Scenario 1, preventing unauthorized traffic from entering via the VPN tunnel. Additionally, a dedicated firewall should be placed between the machine and the production network to closely manage and control data flows in both directions. Ideally, traffic should primarily flow outward from the machine to the plant network, but the firewall can also be configured to selectively permit only specific traffic types from authorized sources into the machine.



[13] Note that according to SP.03.02 RE(2), “For some, responsibility for maintaining firewall rules and documentation transfers to the asset owner prior to or at automation solution turnover. In this case, the service provider’s role may be, as required by the asset owner, only to support verification that the firewall rules are accurate and up-to-date.”

(4) Scenario 4: larger machine with different control systems and connected to a production plant

For complex machines consisting of various types of nodes, risk analysis often indicates the need for additional segmentation within the machine itself. Machine builders should reference the ISA/IEC 62443-3-3 standard to demonstrate maturity and security in their system architectures to their customers. Requirements specifically towards Segmentation and Traffic control to achieve SL1 are:

<table>
<tr><td>Standard</td><td>ISA/IEC 62443-3-3</td></tr>
<tr><td>System Requirement</td><td>SR 5.1</td></tr>
<tr><td>Applies to</td><td>The system configuration</td></tr>
<tr><td colspan="2"><b>Network segmentation according to Security Level 1:</b> the control system shall provide the capability to logically segment control system networks from non-control system networks, and to logically segment critical control system networks from other control system networks.</td></tr>
</table>

<table>
<tr><td>Standard</td><td>ISA/IEC 62443-3-3</td></tr>
<tr><td>System Requirement</td><td>SR 5.2</td></tr>
<tr><td>Applies to</td><td>The system configuration</td></tr>
<tr><td colspan="2"><b>Network segmentation policy according to Security Level 1:</b> the control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.</td></tr>
</table>

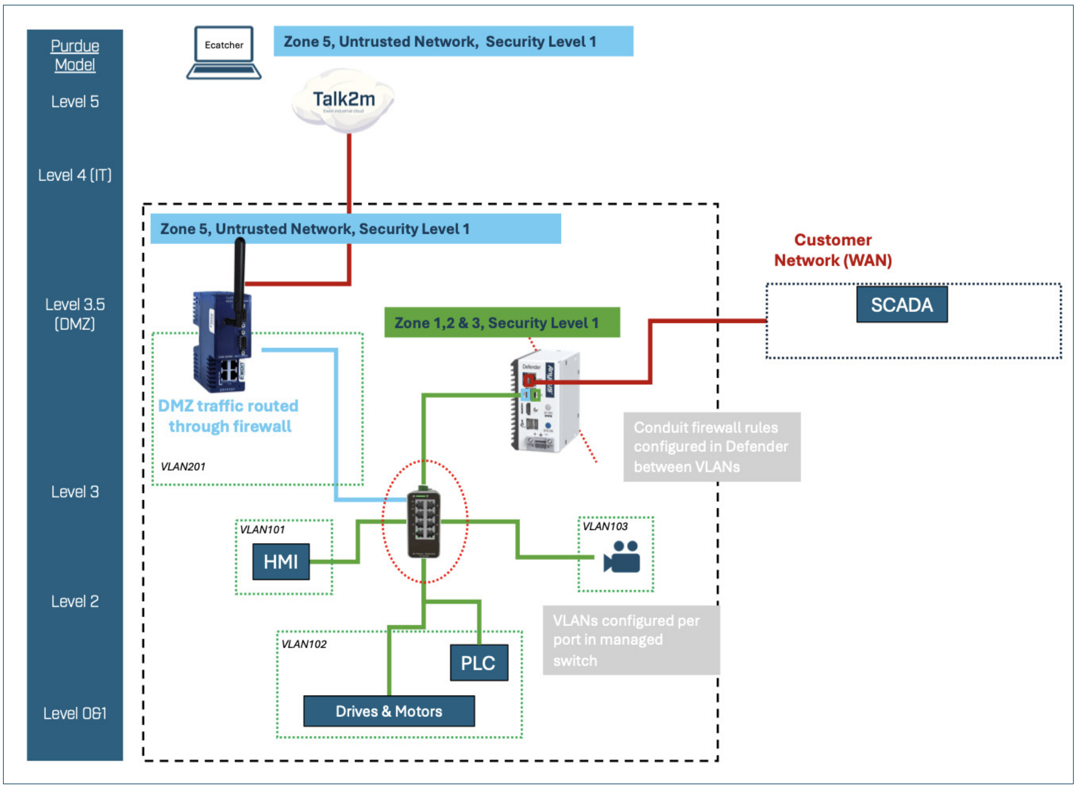
How to implement in the machine and configure an Ewon gateway

The Ewon gateway alone cannot achieve comprehensive network segmentation across multiple segments. To fulfill Security Level 1 (logical segmentation) requirements, deploying VLAN technology is needed. A managed network switch, configured with proper authentication, assigns individual ports to specific VLANs. This effectively prevents direct communication between devices on separate VLANs, logically isolating network segments.

A firewall acting as a conduit is necessary for managing communications between segmented zones or external networks. This firewall must support VLANs and connect via a trunk port on the managed switch, enabling it to interface with all configured VLANs. Traffic between VLANs must pass through the firewall, which provides optimal visibility for monitoring network activity and enforcing traffic control policies.

Depending on the organization's risk tolerance, the Ewon gateway should ideally be placed within its own isolated network segment, separate from critical control components. This setup ensures a clear and controlled communication pathway, effectively managing traffic to and from potentially untrusted remote networks.

If isolating the Ewon gateway in its own segment within the machine isn't feasible, operators must enable the cloud firewall and implement strict access control rules.


Purdue Model
Level 5
Level 4 (IT)
Level 3.5 (DMZ)
Level 3
Level 2
Level 0&1
Ecatcher
Zone 5, Untrusted Network, Security Level 1
Talk2m
Zone 5, Untrusted Network, Security Level 1
Customer Network (WAN)
SCADA
Zone 1,2 & 3, Security Level 1
DMZ traffic routed through firewall
VLAN201
Conduit firewall rules configured in Defender between VLANs
VLAN101
HMI
VLAN103
VLANs configured per port in managed switch
VLAN102
PLC
Drives & Motors

(5) Scenario 5: a larger operational machine

For machines that resemble a small factory by themselves, with several sub-processes that each have their own risk profile, it may be appropriate to apply Security Target level 2 according to the ISA/IEC 62443 model. Example is a machine with a critical processing part (think food processing) and then an annex doing package handling. In addition, a camera network may be deployed to provide visual surveillance.

Standard	ISA/IEC 62443-3-3
System Requirement	SR 5.1 RE 1
Applies to	The system configuration
Physical network segmentation according to Security Level 2: the control system shall provide the capability to physically segment control system networks from non-control system networks and to physically segment critical control system networks from non-critical control system networks.	

Standard	ISA/IEC 62443-3-3
System Requirement	SR 5.2 RE 1
Applies to	The system configuration
Network segmentation policy according to Security Level 2: the control system shall provide the capability to deny network traffic by default and allow network traffic by exception *(also termed deny all, permit by exception).*	

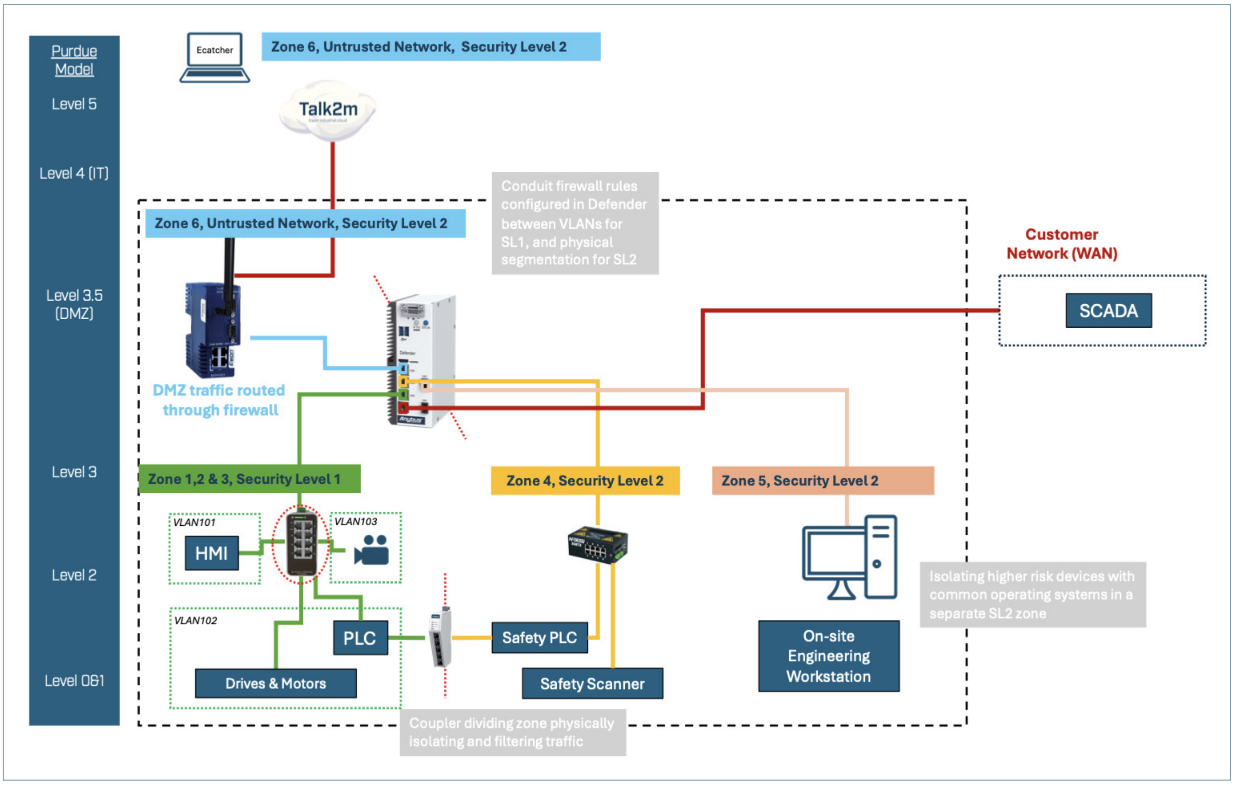
How to implement in the machine and configure an Ewon gateway

The Ewon gateway alone cannot provide comprehensive network segmentation across multiple segments. To meet Security Level 2 (physical segmentation) requirements, the network infrastructure requires a firewall with multiple interfaces separating each zone/segment.

The Control zone must be separated from Safety zones, Untrusted zones and Supervisory zones, such as the engineering workstations. As the Firewall conduit has specific separated network interface cards for each zone the separation will meet Level 2 and higher requirements. The architecture can be combined with a managed network switch configured with appropriate authentication strategies assigns specific ports to specific VLANs, providing level 1 zone separation in the same architecture.

For communication between zones, a strict deny-by-default firewall configured is required, meaning that at least Source IP, Destination IP and Destination Port and Protocol Type must be specified for the traffic flows authorized.

The Ewon gateway should reside in its own isolated physically network segment separates from critical control components. This configuration establishes a clear conduit on-premises, effectively controlling traffic to and from less trusted remote zones.



Conduit firewall rules configured in Defender between VLANs for SL1, and physical segmentation for SL2

Isolating higher risk devices with common operating systems in a separate SL2 zone

Coupler dividing zone physically isolating and filtering traffic

3.9 SECURITY PATCH MANAGEMENT

Category: Network Security

Why it matters?

A patch management policy reduces the risk to industrial systems. Unaddressed vulnerabilities can lead to successful cyberattacks with consequences far beyond data loss or downtime. These incidents can severely disrupt critical industrial processes and compromise safety. To mitigate these risks, timely and effective patch management is essential. It plays a key role in preserving the security, reliability, and resilience of Industrial Automation and Control Systems (IACS). By prioritizing patch management, organizations can defend against evolving threats and ensure the continuous, safe operation of their industrial environments.

What to do according to ISA/IEC 62443

Standard	ISA/IEC 62443-2-4
Req ID	SP.11.01 to SP.11.06
Applies to	The service provider
Service providers must have documented reviewable processes for evaluating and applying security patches relevant to industrial automation solutions. This processes requires that patches be tested, approved, and delivered through the authorized channels to ensure integrity and reduce risk. Service providers must inform asset owners about patch results within an agreed timeframe and recommend mitigation for uninstalled patches. Modified or enhanced software libraries must be handled carefully, with tailored patch procedures. Patch installation must only occur with the asset owner's explicit approval. Clear instructions must be provided for patch installation from various media sources. All patching must be aligned with operational schedules to avoid process disruption.	

Also, the ISA-TR62443-2-3 technical report, titled "Patch Management in the IACS Environment" offers in-depth guidance tailored to the unique challenges of patching within Industrial Automation and Control Systems. It provides a structured approach to designing, implementing, and maintaining effective patch management practices that align with the operational and security needs of industrial environments.

How to configure an Ewon gateway

It is possible to keep all the Ewon devices up to date remotely using the Talk2m Firmware Management feature in Ecatcher[14]

With the Firmware Management feature, account administrators can:

1. Quickly see which Ewon gateway needs security updates or are running on older firmware versions.

- Apply filters to display only those gateways that can have security patches or newer firmware versions applied.
- Icons in the Firmware column identify gateways in need of special attention.

2. Control which firmware versions are applied.

3. Some organizations require new firmware to be internally qualified before being applied.

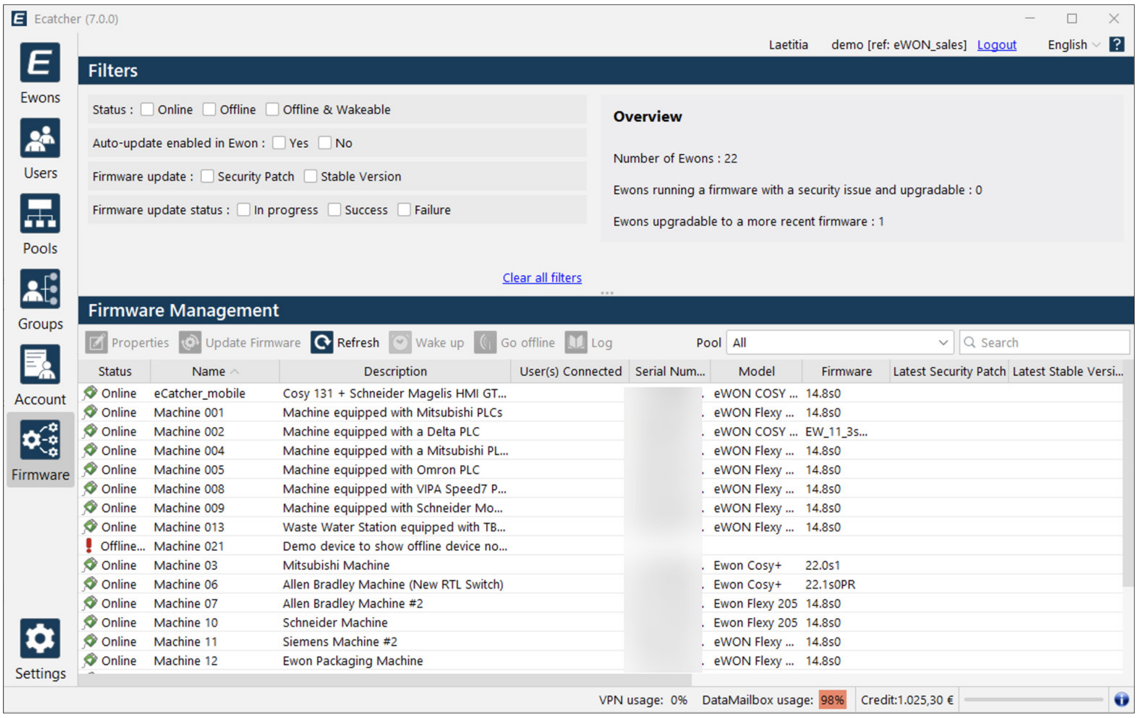
4. With the Firmware Management feature, you can apply the latest firmware version or a specific earlier firmware version.

5. Update the firmware of multiple Ewon gateways at the same time.

6. You can quickly protect all your equipment when new security patches become available.

7. Control when firmware updates are applied.

8. Administrators can apply updates at times when the reboot associated with a firmware update will not interfere with normal operations.



Laetitia demo [ref: eWON_sales] Logout English

Filters

Status : □ Online □ Offline □ Offline & Wakeable

Auto-update enabled in Ewon : □ Yes □ No

Firmware update : □ Security Patch □ Stable Version

Firmware update status : □ In progress □ Success □ Failure

Clear all filters

Overview

Number of Ewons : 22

Ewons running a firmware with a security issue and upgradable : 0

Ewons upgradable to a more recent firmware : 1

Firmware Management

Pool: All

Status	Name	Description	User(s) Connected	Serial Num...	Model	Firmware	Latest Security Patch	Latest Stable Versi...
Online	eCatcher_mobile	Cosy 131 + Schneider Magelis HMI GT...		[redacted]	eWON COSY ...	14.8s0		
Online	Machine 001	Machine equipped with Mitsubishi PLCs		[redacted]	eWON Flexy ...	14.8s0		
Online	Machine 002	Machine equipped with a Delta PLC		[redacted]	eWON COSY ...	EW_11_3s...		
Online	Machine 004	Machine equipped with a Mitsubishi PL...		[redacted]	eWON Flexy ...	14.8s0		
Online	Machine 005	Machine equipped with Omron PLC		[redacted]	eWON Flexy ...	14.8s0		
Online	Machine 008	Machine equipped with VIPA Speed7 P...		[redacted]	eWON Flexy ...	14.8s0		
Online	Machine 009	Machine equipped with Schneider Mo...		[redacted]	eWON Flexy ...	14.8s0		
Online	Machine 013	Waste Water Station equipped with TB...		[redacted]	eWON Flexy ...	14.8s0		
Offline...	Machine 021	Demo device to show offline device no...		[redacted]				
Online	Machine 03	Mitsubishi Machine		[redacted]	Ewon Cosy+	22.0s1		
Online	Machine 06	Allen Bradley Machine (New RTL Switch)		[redacted]	Ewon Cosy+	22.1s0PR		
Online	Machine 07	Allen Bradley Machine #2		[redacted]	Ewon Flexy 205	14.8s0		
Online	Machine 10	Schneider Machine		[redacted]	Ewon Flexy 205	14.8s0		
Online	Machine 11	Siemens Machine #2		[redacted]	eWON Flexy ...	14.8s0		
Online	Machine 12	Ewon Packaging Machine		[redacted]	eWON Flexy ...	14.8s0		

VPN usage: 0% DataMailbox usage: 98% Credit:1.025,30 €

Also note that up-to-date security advisories, as well as options to report vulnerabilities or incidents, can be found on the HMS Security pages.[15]

[14] Function available only in Talk2m pro

[15] https://www.hms-networks.com/cyber-security

3.10 DEACTIVATE UNNEEDED CONNECTIONS AND SERVICES

Category: Network security

Why it matters?

System hardening is an essential process aimed at fortifying a system by significantly reducing its attack surface, or the number of potential avenues for cyber threats. This proactive approach minimizes vulnerabilities by systematically disabling unnecessary services, enforcing robust authentication mechanisms, and regularly applying security patches.

By implementing these practices, system hardening not only enhances the overall security posture but also helps to ensure operational continuity. It effectively minimizes the attack surface, making it more challenging for unauthorized users to gain access.

What to do according to ISA/IEC 62443

Standard	ISA/IEC 62443-2-4
Req ID	SP.03.05
Applies to	The service provider

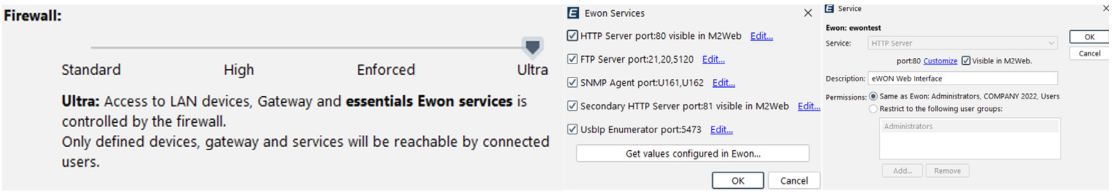
Only software and hardware features required by the automation solution or approved by the asset owner are enabled. At a minimum, this includes ensuring that:

1. Unnecessary software applications and services (e.g. email, office applications, games) and their associated communication access points (e.g. TCP/.UDP ports), USB devices (e.g. mass storage), Bluetooth and wireless communications are disabled and/or removed unless required by the automation solution.
2. Network addresses in use are authorized,
3. Physical and logical access to diagnostic and configuration ports is protected from unauthorized access and use.
4. Unused ports on network devices (e.g. switches and routers) are configured to prevent unauthorized access to the automation solution’s network infrastructure.
5. Maintenance processes maintain the hardened state of the automation solution during its lifetime. The service provider shall ensure that the automation solution is configured to write all security-related events, including user activities and account management activities, to an audit log that is kept for the number of days specified by the asset owner.

Standard	ISA/IEC 62443-3-3
System Requirement	SR7.7
Applies to	The system configuration

The control system shall prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services.

How to configure Ewon

Talk2m	The access to LAN devices, Ewon gateways and essential services is controlled by the included firewall. When the highest firewall level is applied (Ultra), it is possible to limit access to the services of the Ewon gateway itself.  **Firewall:** Standard High Enforced Ultra **Ultra:** Access to LAN devices, Gateway and **essentials Ewon services** is controlled by the firewall. Only defined devices, gateway and services will be reachable by connected users. Ewon Services ☑ HTTP Server port:80 visible in M2Web Edit... ☑ FTP Server port:21,20,5120 Edit... ☑ SNMP Agent port:U161,U162 Edit... ☑ Secondary HTTP Server port:81 visible in M2Web Edit... ☑ UsbIp Enumerator port:5473 Edit... Get values configured in Ewon... OK Cancel Service **Ewon: ewontest** Service: HTTP Server port:80 Customize ☑ Visible in M2Web. Description: eWON Web Interface Permissions: ● Same as Ewon: Administrators, COMPANY 2022, Users ○ Restrict to the following user groups: Administrators Add... Remove OK Cancel
Ewon Flexy	It is possible to block all the unused services/servers like HTTP, FTP, IP-to-Serial, both in LAN and WAN This can be needed when, for instance, HTTP and FTP servers cannot be used onsite because not matching the onsite security policies. So, it is possible to complete block the access to the Ewon Flexy GUI at a local level. For detail information visit https://support.hms-networks.com/hc/en-us/articles/19393244940818-How-to-block-all-the-unused-Ewon-Flexy-Cosy131-services-on-the-LAN-WAN-and-or-VPN-interface

3.11 PROTECTION AGAINST UNAUTHORIZED SOFTWARE

Category: Network security

Why it matters?

By ensuring that only verified firmware run on systems, organizations can enhance their overall cybersecurity posture, protect sensitive data, and uphold the reliability and integrity of both industrial and business operations.

What to do according to ISA/IEC 62443

Standard	ISA/IEC 62443-2-4
Req ID	SP.10.05
Applies to	The service provider
This requires that all devices supplied are free of known malware prior to use in the automation solution.	

Standard	ISA/IEC 62443-3-3
System Requirement	SR3.2
Applies to	The system configuration
This requires the capability to employ protection mechanisms to prevent, detect, report and mitigate the effects of malicious code or unauthorized software.	

How to configure an Ewon gateway

Ewon protects any firmware files in a safe download website. Critical files are securely monitored on HMS website and any changes of the files triggers a notification to the relevant people in the company.

Ewon Cosy+ incorporates an embedded secure element chip which:

- Securely stores and generates secrets (“birth certificate”).
- Provides a root-of-trust at the IC level, for end-to-end security.
- Ensures a secure boot sequence.
- Tamper-resistance to protect against local attacks.

The Secure Element of the Ewon Cosy+ is certified common criteria EAL 6+.

3.12 ALLOW ACCESS TO THE NETWORK ONLY TO AUTHORIZED DEVICES

Category: Network Security

Why it matters?

Unauthorized devices pose significant threats to the integrity and security of organizational systems. They can introduce harmful malware, disrupt essential processes, or be exploited by malicious actors to gain control over critical infrastructure. To safeguard against these risks, it is vital for organizations to implement stringent access controls. This includes utilizing robust authentication mechanisms, enforcing network segmentation, and adopting device whitelisting practices.

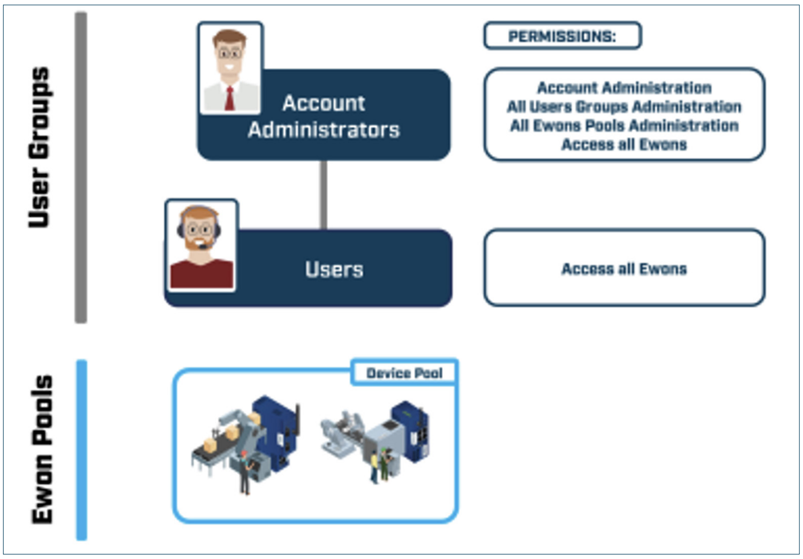
What to do according to ISA/IEC 62443

Standard	ISA/IEC 62443-2-4
Req ID	SP.03.08 RE(3)
Applies to	The service provider
Ensure that access controls used for the administration of network gateways include mutual authentication.	

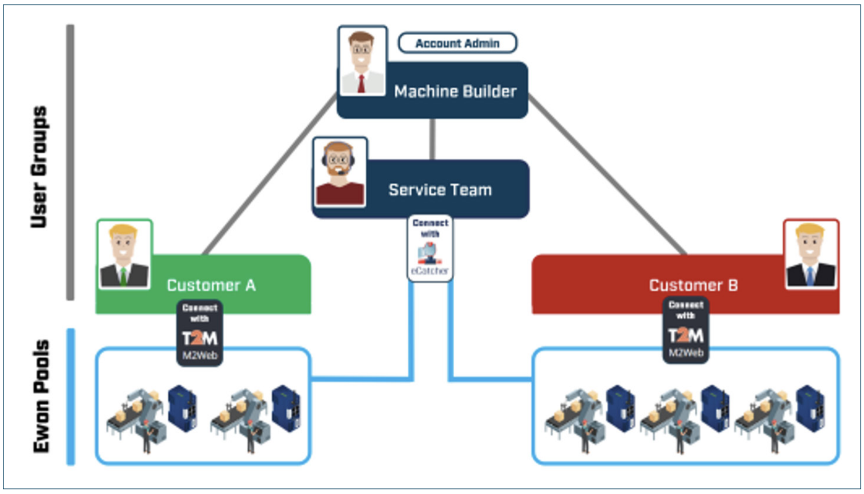
Standard	ISA/IEC 62443-3-3
System Requirement	SR1.2
Applies to	The system configuration
Identify and authenticate all software processes and devices. This capability shall enforce such identification and authentication on all interfaces which provide access to the control system to support least privilege in accordance with applicable security policies and procedures.	

How to configure an Ewon gateway

User groups and Ewon pools are used with a Talk2m pro account to define which users have access to specific Ewon gateways and what permissions they have on Ewon pools and other user groups. By default, a Talk2m pro account includes two user groups: one with full permission and access to all Ewon gateways, and another with access to Ewon gateways in the default Ewon pool.



User groups and Ewon pools can be used to create more complex access rights. For example, within a company, the company's service organization might need its engineers to be able to access any Ewon gateway at any site. Within that organization, though, only the service managers should be able to add or delete Ewon gateways to the account or grant or revoke access rights to their engineers. In addition, the company might want to allow users at each site to have access to view the KPIs from the Ewon gateways at their own locations but only through M2web. By creating multiple and granting appropriate permissions to each group, the company can make sure that users only access the equipment for which they have authorization.



For more information, visit https://hmsnetworkstest.blob.core.windows.net/www/docs/librariesprovider10/downloads-monitored/manuals/user-manuals/um-0005-00-user-manual-Talk2m-pro.pdf

3.13 ESTABLISH, IMPLEMENT AND APPLY A POLICY AND PROCEDURES RELATED TO CRYPTOGRAPHY

Category: Policies & Procedures

Why it matters?

By establishing clear encryption standards, key management practices, and robust authentication mechanisms, these policies provide a framework for safeguarding sensitive information.

Proper implementation of cryptographic measures not only ensures compliance with industry regulations and best practices, but also upholds the integrity, availability, and confidentiality of systems. This comprehensive approach reinforces the security posture of organizations, enabling them to effectively combat evolving cyber threats.

What to do according to ISA/IEC 62443

Standard	ISA/IEC 62443-2-4
Req ID	SP.07.04 RE(1)
Applies to	The service provider
Ensure that all remote access connections conducted over the Internet that are used to support remote access are authenticated and encrypted.	

About Ewon

Ewon Remote access VPN sessions are end-to-end encrypted using SSL/TLS protocol. Communications between the remote user and the Ewon gateway are fully encrypted using the SSL/TLS protocol, thereby ensuring data authenticity, integrity & confidentiality.

3.14 APPLICATIONS USED IN THE AUTOMATION SOLUTION ARE COMMONLY ACCEPTED BY BOTH THE SECURITY AND INDUSTRIAL AUTOMATION COMMUNITIES

Category: Policies & Procedures

Why it matters?

Utilizing applications that are widely recognized and accepted by both the security and industrial automation sectors is essential for guaranteeing reliability, safety, and compliance in automation solutions. These applications undergo thorough vetting for cybersecurity vulnerabilities, and are crafted to adhere to stringent industry standards, effectively mitigating the risks associated with cyber threats and operational disruptions.

Moreover, these applications promote interoperability across various systems, streamline maintenance processes, and ensure adherence to regulatory requirements. By embracing applications that have gained broad acceptance, organizations can significantly bolster their security measures, reduce downtime, and enhance overall efficiency in their automation workflows. This approach not only safeguards critical operations but also fosters a more resilient and productive environment for all stakeholders involved.

What to do according to ISA/IEC 62443

Standard	ISA/IEC 62443-2-4
Req ID	SP.07.01
Applies to	The service provider
Ensure that remote access applications used are commonly accepted by both the security and industrial automation communities.	

About Ewon

Ewon by HMS Networks is the most extended solution for remote access to industrial assets and widely accepted by both the security and industrial automation communities. Since Talk2m first version in 2006, actually more than 500,000 industrial machines are connected to it.

Ewon solution is ISO 27001 certified. This certification ensures top-tier security for remote access and data collection, and is one of the best-known standards in the IT sector. It provides requirements for an information security management system (ISMS) which allows Ewon to implement the following actions:

- **Compliance with the latest regulations**

In May 2018, the General Data Protection Regulation (GDPR) entered into force. Considerable changes had to be made to many systems to guarantee the protection of personal data. Given its strict framework, ISO 27001 certification enables to comply with this legislation quickly.

- **Ensure the level of training of Ewon employees in cybersecurity**

The latest report published by the CNIL in France emphasizes that each year, 46% of IT security incidents affecting businesses are caused by the employees of the companies concerned. The ISO 27001 standard raises awareness of the risks associated with cyberattacks. Per the precepts of this certification, HMS Networks employees are regularly audited and must follow a training program. Both these actions are additional proofs of our commitment to developing secure solutions.

- **Risk Management**

Security is nothing if it does not relate to the most critical processes of an organization. It is imperative to protect your assets effectively. An objective that remains within Ewon grasp through the adoption of sound risk governance. To achieve this, HMS Networks organization must uniformly assess each risk and balance them effectively. The ISO 27001 standard requires the implementation of quantitative and qualitative risk assessment and treatment systems.

HMS Networks is partners with the company NVISO[16] to enhance cybersecurity. NVISO conducts regular security assessments of Ewon systems and provides continuous feedback to strengthen their defenses. This partnership complements Ewon's ISO 27001 certification, ensuring that Ewon products and services remain secure at the highest level - delivering robust protection for remote access to industrial machines.

[16] https://www.nviso.eu/

3.15 DETERMINE AND APPLY CONTROLS FOR REMOTE ACCESS TO IACS

Category: Policies & Procedures

Why it matters?

Remote access enhances efficiency in monitoring, diagnostics, and maintenance but also introduces cybersecurity risks that require a robust security framework. Implementing strict controls over the installation, configuration, operation, and termination of remote access applications is essential to effectively mitigate these risks.

What to do according to ISA/IEC 62443

Standard	ISA/IEC 62443-2-4
Req ID	SP.07.02
Applies to	The service provider
Provide detailed instructions for the installation, configuration, operation, and termination of the remote access applications.	

To fulfill asset owners' requirements according to ISA/IEC 62443-2-1, take into consideration to document for each connection at least the following:

a) The purpose of the remote access connection.

b) The Ewon gateway used for the connection.

c) Encryption and authentication technologies used.

d) The use of Talk2m service cloud-based service.

e) The circumstances requiring the connection. The length of time the connection needs to be open, including expected inactivity periods.

f) The location and identity of the remote client device, application and user, and

g) Any compliance requirements that need to be met prior to establishing the connection.

3.16 REGULARLY REVIEW THE IDENTITIES AND, IF NO LONGER NEEDED, DEACTIVATE THEM WITHOUT DELAY

Category: Policies & Procedures

Why it matters?

Unused or outdated accounts present a considerable security vulnerability, as they can be targeted by malicious actors seeking unauthorized access. It is crucial for organizations to perform regular identity reviews to ensure that only authorized personnel maintain access to their systems. This proactive approach not only mitigates the risk of insider threats but also helps prevent external breaches. By implementing these periodic assessments, organizations can effectively safeguard their assets and maintain a robust security posture.

What to do according to ISA/IEC 62443

Standard	ISA/IEC 62443-2-4
Req ID	SP.09.03
Applies to	The service provider
Ensure that unused system default accounts have been removed or disabled.	

3.17 MAINTAIN POLICIES FOR MANAGEMENT OF PRIVILEGED AND SYSTEM ADMINISTRATION ACCOUNTS

Category: Policies & Procedures

Why it matters?

Ensuring robust policies for managing privileged and system administration accounts within Industrial Control Systems (ICS) is crucial for enhancing security, achieving compliance, and maintaining operational stability. These accounts possess extensive access rights, rendering them prime targets for cyber threats.

What to do according to ISA/IEC 62443

Standard	ISA/IEC 62443-2-4
Req ID	SP.09.01
Applies to	The service provider
Ensure that the solution supports: 1. The use of a single, integrated database, which may be distributed or redundant, for defining and managing user and service accounts. 2. Restricted management of accounts to authorized users. 3. Decentralized access to this database for the management of accounts. 4. Decentralized enforcement of the account settings (e.g. passwords, operating system privileges, and access control lists) defined in this database.	

Standard	ISA/IEC 62443-3-3
System Requirement	SR1.3
Applies to	The system configuration
Provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts.	

4. Conclusion

Secure remote access to industrial environments requires a **multi-layered approach** that combines **strong authentication, network segmentation, encryption, continuous monitoring, and compliance with industry standards like NIS2.**

Machine builders can leverage **cloud-based secure access solutions** to bridge remote connections securely while maintaining **NIS2 compliance** and addressing the security concerns of asset owners.

Organizations must **prioritize security** while ensuring remote access enhances operational efficiency without compromising resilience.

For a tailored security strategy, organizations should conduct **regular risk assessments** and implement **advanced remote access solutions** designed specifically for industrial environments.

Annex A - Mapping of NIS2 to IEC62443 and NIST

Chapter	Category	Measure	NIS2 Article 21	IEC62443-2-1	IEC62443-2-4	IEC62443-3-3	NIST SP800-53v5
3.1	Access Controls	Ensure the strength of authentication is appropriate	(g) basic cyber hygiene practices and cybersecurity training;	USER1.11	SP.09.05	SR1.7	PR.IA-12
3.2	Access Controls	Use Multi-factor authentication	(j) the use of Multi-Factor Authentication (MFA) or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.’	USER1.9	SP.03.07 RE(1)	SR1.1 RE(2)	PR.IA-2
3.3	Access Controls	Change of authentication credentials initially	(g) basic cyber hygiene practices and cybersecurity training;	USER1.1	SP.09.07	SR1.5	PR.AC-1
3.4	Access Controls	Implement authentication procedures based on least privilege principle	(i) human resources security, access control policies and asset management;	USER1.5	SP.03.08	SR2.1	PR.AC-6
3.5	Access Controls	Require the reset of authentication credentials and the blocking of users after a predefined number of unsuccessful log-in attempts	(g) basic cyber hygiene practices and cybersecurity training;	USER1.15	----	SR1.11	PR.AC-7
3.6	Access Controls	Ensure that it obtains approval from the asset owner prior to using each and every remote access connection	(g) basic cyber hygiene practices	NET3.2	SP.07.04	SR1.13 RE(1)	PR.AC-3
3.7	Incident Handling	Use tools to monitor and log activities	(b) incident handling;	EVENT1.6	SP.08.02	SR2.8	PR.AU-2
3.8	Network Security	Network Segmentation	(e) security in network and information systems acquisition	NET1.1	SP.03.02 RE(2)	SR5.1 SR5.2 (with RE)	PR.AC-4
3.9	Network Security	Security patch management	(g) basic cyber hygiene practices	COMP3.2	SP11.xx	----	----
3.1	Network Security	Deactivate unneeded connections and services	(g) basic cyber hygiene practices	COMP1.1	SP.03.05	SR7.7	PR-CM-6
3.11	Network Security	Protection against unauthorized software	(g) basic cyber hygiene practices	COMP2.1	SP.10.05	SR3.2	PR-PS-05
3.12	Network Security	Allow access to the network only to authorized devices	(e) security in network and information systems acquisition	USER 1.19	SP.03.08 RE(3)	SR1.2	PR.IA-3
3.13	Policies & Procedures	Establish, implement and apply a policy and procedures related to cryptography	(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;	DATA1.5	SP.07.04 RE(1)	SR4.3	AC-17(2)
3.14	Policies & Procedures	Applications used in the automation solution are commonly accepted by both the security and industrial automation communities	(g) basic cyber hygiene practices	----	SP.07.01	----	----
3.15	Policies & Procedures	Provide detailed instructions for the installation, configuration, operation, and termination of the remote access	(g) basic cyber hygiene practices	NET3.2	SP.07.02	SR1.13	PR.AC-17(1)
3.16	Policies & Procedures	Regularly review the identities and, if no longer needed, deactivate	(g) basic cyber hygiene practices	USER1.2	SP.09.03	SR1.3	PR.AC-2(3)
3.17	Policies & Procedures	Maintain policies for management of privileged and system administration accounts	(i) human resources security, access control policies and asset management;	USER1.1	SP.09.01	SR1.3	PR.AC-2(7)

Work with HMS Networks.
The number one choice for
industrial communication
and IIoT.

Anybus® BY HMS NETWORKS

Ewon® BY HMS NETWORKS

N-Tron® BY HMS NETWORKS

RedLion® BY HMS NETWORKS

hms-networks.com